UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **KEITHMHELMER@HOTMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 5:21-mj-00012

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, William D. Ruley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Microsoft Corporation, an email provider headquartered at 1 Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of the Interior, Office of Inspector General ("DOI OIG") since August 2015. Prior to that I was a Special Agent with the U.S. Army Criminal Investigation Division, Major Procurement Fraud Unit, a position that I have held since July 2012. I am assigned to the Eastern Region Investigation Office, located in Herndon, Virginia.

As a Special Agent for the DOI OIG, my duties include investigating crimes, including but not limited to contract and grant fraud, false statements, false claims, bribery, and money laundering. I have personally participated in the execution of search warrants and seizing of evidence, including computers and other electronic equipment, from both businesses and personal residences. I am also an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

3. I am currently assigned to an investigation involving allegations of bid rigging and fraud on a contract awarded by the National Park Service ("NPS"). This investigation is within the criminal law enforcement jurisdiction of the DOI OIG.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 15 U.S.C. § 1 (Sherman Act); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. §§ 1343 and 1346 (Wire Fraud and Honest Services Fraud) have been committed by **KEITH HELMER** and **LARRY EPPARD**. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. The Department of the Interior, Office of Inspector General received an anonymous complaint on August 30, 2019 that a subcontractor providing paving services, S.L. Williamson (acting through its Vice President, Larry Eppard), conspired with Keith Helmer to rig National Park Service ("NPS") construction contract bids at Shenandoah National Park for many years.

8. Through document review and witness interviews at one or more of the relevant companies, I have discovered that, since 2015, Helmer has been employed by three general contractors all providing services to NPS: Summit Construction, ITM4G, and Blue Construction Services. Eppard has been the Vice President of S.L. Williamson since at least 2015.

9. As a result of DOI OIG subpoenas, we obtained email communications between SAW Contracting and S.L. Williamson.

10. The investigation thus far has revealed at least one instance of possible bid rigging or fraud in 2018:

a. NPS posted a pavement management services solicitation for the project at issue on **February 20, 2018**.

b. Helmer was employed at Summit Construction when the project solicitation was posted. Eppard was employed at S.L. Williamson.

c. Two of the companies that submitted bids to serve as prime contractors for this NPS project were Summit Construction and SAW Contracting.

d. Eppard, of S.L. Williamson, submitted subcontracting bids to Helmer for both Summit Construction and SAW Contracting.

e. Initially, Eppard sent Helmer identical bids for the two companies.

i. On July 19, 2018, at 7:53am, Eppard emailed Helmer at

keithmhelmer@hotmail.com with S.L. Williamson's subcontractor paving estimate for Summit Construction totaling $4,004,785.50.

ii. On July 23, 2018, at 2:58pm, Eppard emailed Helmer at **keithmhelmer@hotmail.com** with S.L. Williamson's subcontractor paving estimate for SAW Contracting totaling $4,004,785.50.

f. Later, Eppard sent Helmer another bid for Summit Construction with a higher price.

i. On July 23, 2018, at 3:11pm, Eppard emailed Helmer at **keithmhelmer@hotmail.com** a second S.L. Williamson subcontractor paving estimate for Summit Construction totaling $4,423,657.50.

g. NPS awarded SAW Contracting the contract through the competitive bidding process on September 19, 2018.

h. By providing a higher subcontracting bid for the identical project to Summit Construction, Helmer and Eppard appear to have rigged this NPS construction project bid.

i. On **January 17, 2019**, S.L. Williamson signed a contract to serve as SAW Contracting's subcontractor for the project.

j. SAW Contracting contracted with ITM4G to provide a project manager and superintendent for the project. By the time the contract was awarded, Helmer was employed at ITM4G. Helmer acted as ITM4G's project manager on the contract, and his father, Ryan Helmer, acted as superintendent.

11. I have probable cause to believe that Helmer, Eppard, and S.L. Williamson may have violated 15 U.S.C. § 1 or defrauded NPS in violation of 18 U.S.C. §§ 1343 and 1346 by agreeing to submit an intentionally losing bid from Summit Construction, for the benefit of SAW

Contracting.

12. A preservation request has been sent to Microsoft Corporation.

13. In general, an email that is sent to a Microsoft Corporation subscriber is stored in the subscriber's "mail box" on Microsoft Corporation servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft Corporation servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft Corporation's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

14. In my training and experience, I have learned that Microsoft Corporation provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft Corporation allows subscribers to obtain email accounts at the domain name "hotmail.com," like the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft Corporation. During the registration process, Microsoft Corporation asks subscribers to provide basic personal information. Therefore, the computers of Microsoft Corporation are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft Corporation subscribers) and information concerning subscribers and their use of Microsoft Corporation services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. A Microsoft Corporation subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft Corporation.

In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or

exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

20. Based on the forgoing, I request that the Court issue the proposed search warrant.

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft Corporation. Because the warrant will be served on Microsoft Corporation, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

22. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/William D. Ruley
William D. Ruley, Special Agent
Department of the Interior
Office of the Inspector General

Received by reliable electronic means and sworn and attested to by telephone on this 16th day of March 2021.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email address **KEITHMHELMER@HOTMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at 1 Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 25, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from February 20, 2018 to January 17, 2019**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 15 U.S.C. § 1; 18 U.S.C. § 371; 18 U.S.C. §§ 1343 and 1346; 18 U.S.C. § 287; 18 U.S.C. §1001; and 41 U.S.C. § 51 *et seq*., those violations involving Keith Helmer and Larry Eppard and occurring **from February 20, 2018 to January 17, 2019**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence of and records relating to contract steering, fraud, and bid rigging in connection with National Parks Service construction projects at Shenandoah National Park and elsewhere;

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner and user;

(c) Evidence indicating the states of mind of the email account owner, user, and any co-conspirators and aiders and abettors as they relate to the crimes under investigation;

(d) The identity of the person(s) who created or used the email account, including records that help reveal the whereabouts of such person(s);

(e) Evidence that may identify co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and

(f) Evidence relating to the identity of person(s) who communicated with the email account user about matters relating to the crimes under investigation, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel and contractors assisting in the investigation, who may include, in addition to law enforcement officers and agents from the United States Department of Interior Office of Inspector General ("DOI OIG"), law enforcement officers and agents from other government agencies, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DOI OIG may deliver a complete copy of the disclosed electronic data to the custody and control of law enforcement officers and agents from other government agencies, attorneys for the government, and attorney support staff for their independent review.

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review and, if possible, engage with the privilege holder to resolve privilege determinations. If that is not possible, the government will establish a Filter Team of government attorneys and agents. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of

any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft Corporation, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft Corporation. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft Corporation, and they were made by Microsoft Corporation as a regular practice; and

b. such records were generated by Microsoft Corporation's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft Corporation in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft Corporation, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature